REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-20 are pending.

35 U.S.C. §112

Claims 3, 7, 8-11 are rejected under 35 U.S.C. §112. Applicants respectfully traverse the rejection.

Claim 7 has been amended to recite "a network system having an internal client" and "an external client" providing an antecedent basis for "the internal and external clients." Claims 8-11 depend on base claim 7 and have been rejected based on the antecedent rejection of claim 7. Claim 7 has been amended and provides proper antecedent basis for claims 8-11. Applicants respectfully request that the §112 rejection of claims 7-11 be withdrawn.

Claim 3 has been amended to recite in part "signing the encrypted session key using a private key associated with the one of the endpoints." Basis for this modification is found on page 14, lines 1-8 of the specification. The original recitation of the private key being associated with the "intermediary" was an unintended mistake. Applicants respectfully request that the §112 rejection of claim 3 be withdrawn.

35 U.S.C. §101

Claims 12-18 are rejected under 35 U.S.C. §101 as being directed to non statutory matters. Applicants respectfully traverse the rejection.

Claim 12 is amended to a network system having "an internal device", "an external device" and "an intermediate device". Thus, claim 12, as amended,

recites statutory subject matter. Dependent claims 13-15 are similarly amended. Applicants respectfully request that the §101 rejection of claims 12-15 be withdrawn.

Claim 16 has been amended to state that the recited code is "stored in computer readable media and executable on a processor." This amendment changes the form of claim 16 to the more familiar and acceptable *Beauregard* format. Dependent claims 17 and 18 incorporate these changes by virtue of their dependency on base claim 16. Applicants respectfully request that the §101 rejection of claim 16-18 be withdrawn.

35 U.S.C. §102

Claims 1 and 4 are rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent 5,835,726 to Shwed et al (Shwed). Applicants respectfully traverse the rejection.

The invention concerns a network architecture in which two endpoints communicate via a virtual private network (VPN) on an otherwise public network, such as the Internet, and an intermediary is permitted to inspect the data communication in a secure and trusted manner.

In one implementation, the network architecture has an external client and an internal client that exchange encrypted data over a network. The internal client is coupled to the network via a network access point, such as a firewall/proxy server. All three participants have their own pair of public/private keys. An independent key server holds the public keys for all three participants.

The external and internal clients establish a virtual private network by negotiating a session key used to encrypt data being exchanged between them.

Initially, only the clients know the session key, and not the firewall. To grant the firewall trusted access to the data stream on the VPN, the internal client securely transfers the session key to the firewall. The internal client requests and receives the firewall's public key from the key server and encrypts the session key using the firewall's public key. The internal client then signs the encrypted key by encrypting it using the internal client's private key.

The firewall authenticates the signature by decrypting the message using the internal client's public key (obtained from the key server or directly from the internal computer). The firewall then decrypts the session key using its own private key. If the dual decryption yields a valid key, the firewall is assured that the session key was sent by the internal client and was not subsequently altered or tampered with in route.

Once the session key is transferred, the firewall is able to decrypt the data stream on the VPN. The firewall can now unintrusively inspect the data stream in a manner that is transparent to the external and internal clients. The claims capture this architecture and new technology.

Claim 1 for example recites a "method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption."

The method of claim 1 provides for an establishment of a virtual private network (VPN) between two computers (endpoints) where the computers (endpoints) engage in key negotiation process to negotiate a session key (see specification page 9, lines 11-13). With the session key, the endpoints (internal and external clients) are able to encrypt messages and begin an encrypted communication session directly with one another (see specification page 9, lines 11-17, Fig. 2). Once the session key is created, one of the endpoints is able to securely share the key with the intermediary to permit trusted inspection.

The method of claim 1 is not disclosed by Shwed. Shwed shows host 1 and host 2 computers (also referred to by the Examiner as endpoints) connected to respective private networks. Host 1 and host 2 are secured through respective firewalls. The firewalls connect to one another by way of a public network. See Shwed, col 14, lines 19-39, Fig. 16. Host 1 and host 2 do not directly communicate with one another.

Shwed does not disclose that the host computers use a session key known to each other. Instead, Shwed uses firewalls to generate session keys (see Shwed col. 15, lines 33-36), not the host computers. The firewalls also perform the encryption. This is pointed out by Examiner that "packet filter modules are installed in firewalls where modification, inspection of packets is performed by encryption of outbound packets and decryption of inbound packets." Shwed at col. 13, lines 6-20.

Claim 1 recites "using a session key known to both endpoints" and "securely transferring the session key from one of the endpoints to an intermediary." Shwed is silent as to this feature. Since Shwed's system does not allow the host computers to negotiate a session key, there is no way that one of the

hosts can securely transfer the session key to an intermediary such as a firewall. Shwed shows a shared session key R used by firewall computers, firewall1 and firewall2, but not between host 1 and host 2 computers. (Shwed at col. 16, lines 27-31) Host 1 and host 2 computers in Shwed never see the session key R. In Shwed, session key R is not transferred from *one end point to an intermediary* by encrypting the session key R using a secret common key B. Host 1 and host 2 computers are not involved in a key exchange, never see any of the keys, and therefore would not be able to transfer a session key or any key to an intermediary (firewall). For these reasons, claim 1 is patentable over Shwed.

The Examiner points out that "Shwed teaches that an endpoint in sending a packet M to a receiving endpoint, first it generates a signature on the packet and then encrypts it using a function key of session key R and finally transmits the encrypted packet over the public network to the receiver endpoint" referring to Shwed col. 18, lines 9-46. As discussed, Shwed shows firewalls encrypting packets, not endpoints. Further, in Shwed only the firewalls see the session key R, the host computers never see session key R.

Shwed shows a firewall receiving an encrypted packet and verifies the encrypted packet through decryption of the encrypted packet through decryption of the encrypted packet and verification of the signature. Shwed col. 18, lines 47-67 through col. 19, lines 1-3. This session data exchange is "performed by a firewall in receiving an encrypted packet from another firewall." Shwed col. 18, lines 47-49. The endpoints in Shwed receive "decrypted" packets. Shwed col. 15, lines 5-11. The present invention as recited in claim 1 involves "an encrypted data stream being transferred over a network between two endpoints." As discussed, endpoints computers and intermediary firewall computers are treated as separate entities.

The Examiner in applying Shwed incorrectly treats endpoint computers as being the same as intermediary firewall computers.

For these reasons, claim 1 is patentable over Shwed. Applicants respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claim 4 is allowable by virtue of its dependency on base claim 1. For the reasons given above with respect to claim 1, the systems and methods recited in claim 4 are neither disclosed nor taught by Shwed. Applicants respectfully request that the §102 rejection of claim 4 be withdrawn.

35 U.S.C. §103

Claims 2, 3 and 5-20 are rejected under 35 U.S.C. §103 as being unpatentable over Shwed in view of Bruce Schneier, Applied Cryptography, Second Addition, 1996 (Schneier). Applicants respectfully traverse the rejection.

Claims 2 and 3 depend from claim 1 and hence incorporate the features of claim 1. As such claims 2 and 3 require "securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream; decrypting the encrypted data stream at the intermediary using the session key; and inspecting the data stream following decryption."

Shwed does not suggest nor teach an architecture where a VPN can be established such that two endpoints can share a session key. The session key in Shwed is known only by and between the intermediary firewalls not the endpoint computers. The endpoints in Shwed do not share a common session key nor are they involved in encryption with one another. Thus, Shwed does not suggest nor teach transferring a session key from one of the endpoints to an intermediary as recited in claim 1. Since the intermediary firewalls perform session key exchange

with one another, there would not be a need for an endpoint to transfer the session key to an intermediary. Further, in Shwed, it would be impossible for an endpoint to transfer a session key to an intermediary, since the endpoints never see the session key.

Schneier is cited for its teaching of known cryptosystems, in particular key exchange systems. Schneier provides no assistance as to the recited methodology of claims 2 and 3. Accordingly, a combination of Shwed and Schneier fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 2 and 3 be withdrawn.

Claim 5 defines "a method for inspecting an encrypted data stream being transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints ... passing the signed encrypted session key to the intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach encrypted data streams that are transferred between two endpoints using a session key known to the two endpoints. The Shwed/Schneier combination does not suggest nor teach that a session key be passed from an endpoint to an intermediary. Therefore, even in view of Schneier, claim 5 is not obvious. Applicants respectfully request that the §103 rejection of claim 5 be withdrawn.

Dependent claim 6 is allowable by virtue of its dependency on base claim 5. Applicants respectfully request that the §103 rejection of claim 6 be withdrawn.

Amended claim 7 defines "in a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients ... a

method executed at the firewall comprising receiving an encrypted and signed session key from the internal client." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach that a session key be received by a firewall from an internal client. Applicants respectfully request that the §103 rejection of claim 7 be withdrawn.

Dependent claims 8, 9, 10, and 11 are allowable by virtue of their dependency on base claim 7. Applicants respectfully request that the §103 rejection of claims 8, 9, 10, and 11 be withdrawn.

Claim 12 defines "a network system comprising an internal client and an external client configured to communicate encrypted data over a network ..., the data being encrypted using a session key, the internal client being configured to securely transfer the session key to the intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach that the internal client be configured to transfer such a session key to an intermediary. Applicants respectfully request that the §103 rejection of claim 12 be withdrawn.

Dependent claims 13, 14, and 15 are allowable by virtue of their dependency on base claim 12. Applicants respectfully request that the §103 rejection of claims 13, 14, and 15 be withdrawn.

Claim 16 defines "a software architecture for a network system having two endpoints that exchange encrypted data over a network and through an

intermediary, the encrypted data being encrypted using a session key known to the endpoints comprising: endpoint-resident code stored on computer readable media and executable on a processor to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and intermediary-resident code stored on computer readable media and executable on the processor to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination fails to teach that a session key be known to the endpoints. The Shwed/Schneier combination fails to teach endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary. The Shwed/Schneier combination further fails to teach intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints. Applicants respectfully request that the §103 rejection of claim 16 be withdrawn.

Dependent claims 17 and 18 are allowable by virtue of their dependency on base claim 16. Applicants respectfully request that the §103 rejection of claims 17 and 18 be withdrawn.

Claim 19 defines "a network system having an internal client that exchanges encrypted data with an external client over a network and through a

firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients … passing the signed and encrypted session key to the intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach the session key being passed to the intermediary. Applicants respectfully request that the §103 rejection of claim 19 be withdrawn.

Claim 20 defines "a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints …securely transferring the session key from one of the endpoints to an intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach that the session key be transferred from one of the endpoints to an intermediary. Applicants respectfully request that the §103 rejection of claim 20 be withdrawn.

CONCLUSION

All pending claims 1-20 are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: 10/29/02

By: _____

Emmanuel A. Rivera
Reg. No. 45,760
(509) 324-9256 ext. 245

MARKED UP VERSION OF PENDING CLAIMS UNDER 37 C.F.R. § 1.121(C)(1)(ii):

Amend claim 3, 7, 12-19 as follows and in accordance with 37 C.F.R. § 1.121(c)(1)(ii), by which the Applicant submits the following marked up version only for claims being changed by the current amendment, wherein the markings are shown by brackets (for deleted matter) and/or underlining (for added matter):

3. (Amended Once) A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary;

signing the encrypted session key using a private key associated with the [intermediary]one of the endpoints; and

sending the signed and encrypted session key to the intermediary.

7. (Once Amended) In a network system having an [external]internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a method executed at the firewall comprising:

receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client;

authenticating the digital signature as belonging to the internal client;

decrypting the session key; and

decrypting the encrypted data being exchanged between the internal and external clients using the session key.

12. (Amended Once) A network system comprising:

an internal client device and an external client device configured to communicate encrypted data over a network using virtual private network communication, the data being encrypted using a session key;

an intermediary device having access to the encrypted data being communicated between the internal client device and the external client device;

the internal client device being configured to securely transfer the session key to the intermediary device; and

the intermediary device being configured to decrypt the data using the session key and to inspect the data.

13. (Amended Once) A network system as recited in claim 12, wherein the internal client device encrypts the session key prior to sending it to the intermediary device.

14. (Amended Once) A network system as recited in claim 12, wherein the internal client device encrypts and signs the session key prior to sending it to the intermediary device.

15. (Amended Once) A network system as recited in claim 12, wherein the intermediary device stores the data in unencrypted form.

16. (Amended Once) A software architecture for a network system having two endpoints that exchange encrypted data over a network and through an intermediary, the encrypted data being encrypted using a session key known to the endpoints, comprising:

endpoint-resident code stored on computer readable media and executable on a processor to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and

intermediary-resident code stored on computer readable media and executable on the processor to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints.

17. (Amended Once) A software architecture as recited in claim 16, wherein the intermediary-resident code inspects the data in unencrypted form.

18. (Amended Once) A software architecture as recited in claim 16, wherein the intermediary-resident code stores the data in unencrypted form.

19. (Amended Once) In a network system having an [external]internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, computer-readable media distributed at the internal client and the firewall storing computer-executable instructions for:

encrypting the session key at the internal client;

signing the encrypted session key with a digital signature associated with the internal client;

passing the signed and encrypted session key to the intermediary;

authenticating, at the intermediary, the digital signature of the internal client;

decrypting the session key at the intermediary;

decrypting, at the intermediary, the encrypted data using the session key; and

inspecting the data in route between the internal and external clients.

MARKED UP VERSION OF SPECIFICATION UNDER 37 C.F.R. § 1.121(B)(1)(iii):

Page 10, second paragraph

Fig. 3 shows an exemplary implementation of a computer, such as the external client 42, the internal client 44, firewall [58]48, or key server 66. The host computer is a general-purpose computing device in the form of a conventional personal computer 100 that is configured to operate as a network server (in the case of the firewall and key server computers) or as a client computer (in the case of the external and internal clients).